WHAT IS CLAIMED IS:

1. A method of detecting malicious scripts using code insertion technique, comprising the step of:

checking values related to each sentence belonging to call sequences by using method call sequence detection based on rules including matching rules and relation rules,

wherein the checking step comprises the steps of:

inserting a self-detection routine (malicious behavior detection routine) call sentence before and after a method call sentence of an original script; and

detecting the malicious codes during execution of the script through a self-detection routine inserted into the original script.

2. The method according to claim 1, wherein the self-detection routine call sentence is composed of sentences for storing parameters and return values and calling a detection engine, said sentences being inserted before and after the method call sentence when the method call sentence matches with contents described in the matching rule, and wherein the self-detection routine includes a rule-based detection engine for executing the relation rule related to a relevant matching rule when a method corresponding to the matching rule is called and detecting the presence of malicious behavior of the method call sequence, and methods for causing the parameters and return values of the method call sentence satisfying the matching rule to be stored into a buffer usable by the detection engine.